

REMARKS

No claims have been amended or cancelled by this Response. Claims 2-7, 9-14 and 16-20 are pending in this application.

Claims 2, 9 and 16 stand rejected under 35 U.S.C. §102(a) as being anticipated by Cordery et al. (WO 98/57304). Claims 3, 5-7, 10, 12-14, 17, 19 and 20 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Cordery et al. (WO 98/57304) in view of Cordery et al. (WO 98/57306). Claims 4, 11 and 18 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Cordery et al. (WO 98/57304) in view of Cordery et al. (WO 98/57306) and further in view of Wells et al. (U.S. 2001/0032881). Reconsideration is respectfully requested.

The present invention is directed to a mail piece verification system that can help prevent a fraud by duplication, i.e., generating multiple copies of a single postage indicium. The system includes a plurality of postage metering systems for preparing mail pieces, a plurality of mail processing centers for receiving mail pieces and obtaining the respective mail piece data and a data center in operative communication with the plurality of postage metering systems and the plurality of mail processing centers. The data center includes a plurality of account files corresponding to the plurality of postage metering systems. The data center stores reset data in each of the plurality of account files representative of reset activity (postage purchased) associated with the plurality of postage metering systems. The data center receives respective mail piece data corresponding to the mail pieces from the plurality of mail processing centers, and uses the respective mail piece data to store empirical data in each of the plurality of account files representative of mailing activity (postage consumed) associated with the plurality of postage metering systems. The data center can then conduct a forensic accounting analysis of the empirical data (postage consumed) and the reset data (postage purchased) associated with a selected postage metering system. For example, the reset activity data may be used to ascertain an amount of postage that has been purchased by a respective postage metering system over a given time period. The empirical data may be used to ascertain an amount of postage that has been consumed in relation to the given time period. By comparing the purchased postage amount

with the consumed postage amount, the propriety of the customer's mailing activity may be established. (Specification, page 13, lines 25-31). For example, if a postage metering system purchased only \$100 worth of postage over a given time period, but the amount of postage consumed during the time period, i.e., the amount of postage on mail pieces that have entered the mail stream for delivery that is associated with that postage metering system, totals more \$100, there is a strong indication of fraud by duplication, i.e., a single postage indicium has been copied onto more than one mail piece.

In view of the above, claim 2 is directed to a mail piece verification system that comprises "a data center in operative communication with a plurality of mail processing centers, the data center including a plurality of account files corresponding to a plurality of postage metering systems; and wherein the data center is for: storing reset data in each of the plurality of account files representative of reset activity associated with the plurality of postage metering systems, respectively; receiving respective mail piece data corresponding to the mail pieces from the plurality of mail processing centers; using the respective mail piece data, storing empirical data in each of the plurality of account files representative of mailing activity associated with the plurality of postage metering systems, respectively; and conducting a forensic accounting analysis of the empirical data and the reset data associated with a selected postage metering system using a previously defined time period over which to conduct the forensic accounting analysis."

Cordery et al. (WO 98/57304, hereinafter referred to as Cordery et al. '304), in contrast, is directed to a virtual postage metering system that can be used to generate the evidence of postage. In Cordery et al. '304, digital data security for a Data Center of the virtual postage metering system prevents inadvertent and intentional modifications to meter and user data stored at the Data Center. In Cordery et al. '304 security boxes are used to protect against unauthorized alteration of meter and user records stored at the data center. Cordery et al. '304 also provides secure control of digital token generation process and the associated secure accounting for each postage evidencing transaction occurring at the data center. (page 5, line 32 to page 6, line 6).

According to Cordery et al. '304, a system and method of evidencing postage payment provides a secure box that is used to sign the transaction data and to authenticate meter and user records. The system and method include a data center with a database having a plurality of meter records stored therein. Each meter record includes meter information corresponding to a metering account assigned to each of a plurality of remote user devices that are authorized to request evidence of postage payment. When a request for postage is received at the data center, a secure co-processor device in the data center obtains the appropriate meter record and verifies the authenticity of the meter record by verifying a signature in the meter record and comparing freshness data in the meter record to freshness data in the secure device. If verified, the secure device then accounts for an amount of postage to be evidenced, generating evidence of postage payment and updates the meter information, including the freshness data, in the meter record. The secure device then signs the updated meter information and stores the signature in the meter record. The secure device then returns the updated meter record to the database. (Page 6, line 21 to page 7, line 3).

Thus, Cordery et al. '304 is directed to a virtual postage metering system that allows mailers to use a conventional PC to remotely obtain evidence of postage payment on an as needed basis. The virtual postage metering system does not include any meter hardware at the mailer's site, nor are any funds stored at the mailer's site. All metering and accounting of funds occur at a data center using functional software and database records representing each mailer's "postage meter." (Page 7, line 19 to page 8, line 2). There is no disclosure, teaching or suggestion in Cordery et al. '304 of a mail piece verification system – the system is Cordery et al. '304 is directed to generating the evidence of postage payment before the mail piece is placed into the mail stream for delivery. This is not the same as verifying the evidence of postage payment. This system of Cordery et al. '304 simply generates an indicium for postage evidence – it does not, and can not, determine if a mailer is improperly copying a generated indicium onto multiple mail pieces and reusing the same indicium more than once, since the system in Cordery et al. '304 is in no way related to a verification system.

There is also no disclosure, teaching or suggestion in Cordery et al. '304 of the data center receiving respective mail piece data corresponding to the mail pieces from the plurality of mail processing centers, and using the respective mail piece data, storing empirical data in each of the plurality of account files representative of mailing activity associated with the plurality of postage metering systems as is recited in claim 2. As note above, Cordery et al. '304 is not directed to a verification system that would have access to any empirical data representative of mailing activity, such as, for example, a historical account of observed mailing activity based on the mail pieces that are placed into the mail stream for delivery. The Office Action contends that page 6, lines 1-5 of Cordery et al. '304 discloses these features. Applicant respectfully disagrees. The passage recited by the Office Action from Cordery et al. '304 relates to a transaction request made by a mailer to generate evidence of postage. The mailer has to be authenticated based on records corresponding to the meter account of the mailer initiating the request. Once the mailer has been authenticated, the appropriate meter record can be communicated to the meter box which verifies a signature and freshness data for the record. The meter box then can perform the accounting functions, generate a token for the requested transaction, and generate data for an indicium. Thus, while the system in Cordery et al. '304 will know how much postage was actually purchased by a mailer, there is no way the system in Cordery et al. '304 knows how much mailing activity, i.e., postage consumed, has been performed by the user. The system of Cordery et al. '304 is unable to determine if a specific generated indicium has been used only once (as it should be) or has been improperly copied onto multiple mail pieces and used multiple times, since the system of Cordery et al. '304 is not directed to verification of the indicium. There is simply no disclosure, teaching or suggestion in the system of Cordery et al. '304 of storing empirical data representative of mailing activity as in the present invention.

There is also no disclosure, teaching or suggestion in Cordery et al. '304 of the data center conducting a forensic accounting analysis of the empirical data and the reset postage data associated with a selected postage metering system using a previously defined time period over which to conduct the forensic accounting analysis as is recited in claim 2, since as noted above, the system in Cordery et al. '304 does not have any access to any type of empirical data representative of mailing activity. The Office Action contends that page 6, lines 22-26 of

Cordery et al. '304 discloses this feature. Applicant respectfully disagrees. Page 6, line 15, to page 7, line 4 of Cordery et al. '304 is reproduced below.

Although the digital signature provides reasonable security, it is not bulletproof. It has been found that a historically signed record could be used in place of a current record requiring a more robust verification system to detect such "tampering". In accordance with the present invention, another level of security is added. It has been found that once the signature is verified, the transaction data can be checked for freshness to eliminate any possibility of tampering, inadvertent or intentional.

In accordance with the present invention, a system and method of evidencing postage payment provides a secure box is used to sign the transaction data and to authenticate meter and user records. The system and method includes a data center with a database having a plurality of meter records stored therein. Each meter record includes meter information corresponding to a metering account assigned to each of a plurality of remote user devices that are authorized to request evidence of postage payment. When a request for postage is received at the data center, a secure co-processor device in the data center obtains the appropriate meter record and verifies the authenticity of the meter record by verifying a signature in the meter record and comparing freshness data in the meter record to freshness data in the secure device. If verified, the secure device then accounts for an amount of postage to be evidenced, generating evidence of postage payment and updates the meter information, including the freshness data, in the meter record. The secure device then signs the updated meter information and stores the signature in the meter record. The secure device then returns the updated meter record to the database.

Note that the passage from Cordery et al. '304 cited by the Office Action relates to securing the records for an amount of postage purchased by a user to prevent inadvertent and intentional modifications to meter and user data stored at the Data Center. Thus, while the system in Cordery et al. '304 will know how much postage was actually purchased by a mailer (the reset data), the system of Cordery et al. '304 does not have any access to empirical data representative of mailing activity, i.e., the amount of postage actually consumed. As noted above, a forensic accounting analysis could be performed, for example, by comparing the purchased postage amount (reset data) with the postage actually consumed by the mailer, i.e., the amount of postage on mail pieces that have entered the mail stream for delivery (empirical data). If the amount of postage consumed by the mailer is higher than the amount of postage actually purchased by the mailer, this is a very good indication of fraudulent activity, e.g., copying of indicia onto multiple mail pieces. Since the system of Cordery et al. '304 has no way of knowing

the consumed postage amount, it is impossible for the system of Cordery et al. '304 to conduct any type of accounting analysis, nevertheless one of empirical data representative of mailing activity and reset activity.

For at least the above reasons, Applicant respectfully submits that claim 2 is allowable over the prior art of record.

Each of independent claims 9 and 16 include limitations substantially similar to those of claim 2. For the same reasons claim 2 is allowable, Applicants respectfully submit that claims 9 and 16 are allowable over the prior art of record.

Each of the remaining claims are dependent on one of claims 2, 9 or 16, and therefore include the limitation of the independent claims. The references to Cordery et al. '306 and Wells do not overcome the above deficiencies. Accordingly, Applicant respectfully submits that claims 3-7, 10-14 and 17-20, dependent upon claims 2, 9 and 16, respectively, are allowable along with claims 2, 9 and 16 and on their own merits.

In view of the foregoing remarks, it is respectfully submitted that the pending claims are in a condition for allowance and favorable action thereon is requested.

Respectfully submitted,



Brian A. Lemm
Reg. No. 43,748
Attorney for Applicant
Telephone No.: (203) 924-3836

PITNEY BOWES INC.
Intellectual Property and
Technology Law Department
35 Waterview Drive
P.O. Box 3000
Shelton, CT 06484-8000